KEEPING YOUR CHARITY SAFE IN THE PANDEMIC AND BEYOND

By changing the way many charities must operate, the coronavirus pandemic has created new vulnerabilities which fraudsters and cybercriminals may exploit. This brief guide looks at what they are and how you can respond.

HELPSHEET

Introduction

Fraudsters thrive in crises like the Covid-19 pandemic as well as in the economic difficulties that often accompany them.

For charities large and small the unfamiliar operational and financial challenges, the urgent shift to remote working, the roll-out of new communications technologies and the furloughing of staff have together created significant new fraud vulnerabilities which need to be tackled.

Fraud in the pandemic

Many traditional frauds (such as phishing emails, mandate, procurement, payment diversion and CEO fraud) continue, but with a Covid-19 twist. Scarce vital supplies and services (such as PPE, face masks and vaccines), along with the government's various stimulus and safety net schemes, are all targets.

The sudden shift to reduced and remote working has spread confusion and fear, fertile ground for fraudsters and cybercriminals.

- New and unfamiliar online communication and collaboration tools.
- Increasing social isolation for those still employed.
- Growing financial precariousness for almost everyone else.

With individuals finding themselves under pressure, and with weakened oversight and controls, insider fraud often increases in hard times.

These unprecedented changes in working patterns may be here to stay – the 'new normal' – with long term implications for how charities must assess and manage fraud risk.

Fraud in a downturn

A post-Covid economic downturn promises 12-18 months of new challenges, fresh uncertainties and heightened risk.

- **Insider fraud**: staff and volunteers coming under increasing financial pressure may try to take advantage of financial controls weakened by the pandemic response.
- **Cybercrime (including cyber-fraud)**: in particular, phishing emails, data theft and ransomware attacks will all continue to be key risks for charities.
- **Procurement fraud**: a tougher trading environment may prompt corrupt staff, contractors or suppliers to bribe and collude, manipulating procurement processes to supply goods and services that are shoddy, overpriced or which simply never arrive.
- **Financial statement fraud**: organisations in difficulty – and there will be many – may be tempted to present a façade of solvency by fiddling the books.

And if your charity provides community advice and support, the many 'consumer frauds' – such as investment and courier frauds – will have your beneficiaries and service users as their targets. Always check the **Action Fraud** website for the latest information on these threats.

The fraud triangle

The fraud triangle can help you understand this changing threat landscape and decide how to respond. Its three elements – pressure, rationalisation, opportunity – must all be present for fraud to occur. In times of crisis all three tend to be on the rise.

- **Pressure, motive or incentive**. Money worries and other personal problems are often the motive for fraud.
- **Justification or rationalisation**. The reasons people give for doing what they do. For some, being made redundant after long and loyal service can leave a sense of grievance or the feeling that they are 'owed'. Alternatively, a loyal staff member might act unethically because they think they are helping save the organisation from financial ruin.
- **Opportunity**. The circumstances that make fraud possible and the probability of being caught remote. Dramatic change creates new fraud vulnerabilities. Weakened monitoring and review procedures might struggle to prevent and detect.

HEADLINE FRAUD RISKS IN 2021

1. CYBERCRIME
2. INSIDER (OR STAFF/VOLUNTEER) FRAUD
3. PROCUREMENT FRAUD
4. FINANCIAL STATEMENT FRAUD

CHARITY FRAUD AWARE

CHECKLIST
BUILDING YOUR CHARITY'S DEFENCES

Even in the current, fluid fraud risk environment, the main way to protect your charity is to make sure you have the basics right.

☐ Consider how new ways of working may have affected essential fraud prevention controls and the segregation of duties. Then review regularly. Something fit for purpose now may not be in just a few months' time. Something tolerated temporarily in an emergency may quickly become completely unacceptable.

☐ Make sure you have good, basic cyber-security measures: strong passwords, regular data backups, and software updates performed as soon as they become available.

☐ Check that individual trustees, staff and volunteers understand their own role in preventing fraud and cybercrime. Are they sufficiently knowledgeable to recognise red flags, confident to raise concerns and secure enough to be open about their own mistakes (such as clicking on a dodgy link in a suspicious email)?

☐ Review whistleblowing policies and procedures and try to foster a no-blame culture that prioritises collective learning not punishment.

☐ Start a regular and open dialogue about fraud with your trustees and senior managers and appoint a counter-fraud champion on your board.

☐ Because new ways of working have increased the risk of insider fraud you should review and update your staff recruitment and exit procedures to reflect the changes.

And finally, as you move through and beyond the crisis, and as working practices continue to change, you will need to conduct regular reviews to ensure policies and processes always remain appropriate to the moment and fit for purpose.

OTHER RESOURCES

The UK's National Cyber Security Centre has produced guidance for charities on how to improve cyber security quickly, easily and at low cost. See **'Cyber security: small charity guide'**.

The Charity Finance Group has produced a **counter fraud pledge** for charities to demonstrate their commitment to tackling fraud.

Charity Fraud Awareness Week 2019. **'An introduction to board support for counter fraud'** (helpsheet).

Charity Fraud Awareness Week 2019. **'An introduction to cyber security'** (helpsheet).

Charity Fraud Awareness Week 2018. **'Getting to know your staff'** (helpsheet).

Charity Fraud Awareness Week 2018. **'An introduction to whistleblowing'** (helpsheet).

PRODUCED BY

CANCER RESEARCH UK

CFG INSPIRING FINANCIAL LEADERSHIP

CHARITY COMMISSION FOR ENGLAND AND WALES

FRAUD ADVISORY PANEL

Small Charities Coalition

National Cyber Security Centre a part of GCHQ